

eSecurity News—Summer Vacation

Cyber Security never takes a Vacation!



During the summer months we like to hit the open road, the airport, the cruise ship or other modes of travel for national and international travel. It's important to remember that cyber security threats never take a vacation and neither should our cyber security best practices. Below are tips to stay safe and smart while traveling.

STOP & THINK BEFORE YOU SHARE

- Be careful about how much you post on social media about your vacations before and during your travels. Criminals can, and do, watch online posts to find people that are on vacation because that means you have potentially left your home unattended.
- Before “checking in” to a location on a social network, consider what else you are sharing – like the information that you aren’t home. Consider skipping the “check in” and making your vacation posts after you return home.
- If you do post while you are away use privacy settings that only let friends see your posts.
- If enabled, turn off GPS and auto-tagging and auto-check in features.

PROTECT YOUR DEVICES

Keep your devices (laptop, tablet, or smartphone) with you or with someone you trust. Never leave your device unattended while travelling.

- Set a strong password: Use at least 8 characters in upper and lower case, numbers, and symbols. See [Create a Strong Password](#).
- Set a strong pattern lock: Use at least 7 points and double it back over itself with at least 2 turns. See [How to Secure your Android Phone, with a Pin, Password or Pattern](#).

➔ For more tips visit StaySafeOnline.org

Visit the DTI [eSecurity website](#) for previous issues of
eSecurity Newsletters

DISABLE WI-FI AUTO CONNECT

- Turn off the auto-connect feature that searches for, and automatically connects your device to Wi-Fi networks without your interaction. This could leave you vulnerable to an unencrypted source or one that was set up by a malicious actor to eavesdrop on you.
- Only use secure, encrypted networks. Check with store or hotel employees before connecting to the store/hotel network so you know you are connecting to the correct network and using the correct password for a more secure, encrypted network.
- If the option is available, instead of using public Wi-Fi, use your phone as a Wi-Fi hotspot. Your phone, as a hotspot, provides a more secure connection for another device that can’t make direct use of the cellular network’s connection.
- Do not choose “remember this network” or “join this network automatically” once you have settled on a trusted network for use during your vacation. Generalized network names may connect you to a less secure site that happens to have the same name.



TRAVELING ABROAD?

Visit digiKnow.dti.delaware.gov for tips on international travel.

Questions, comments or topic suggestions?
Email us at eSecurity@state.de.us

